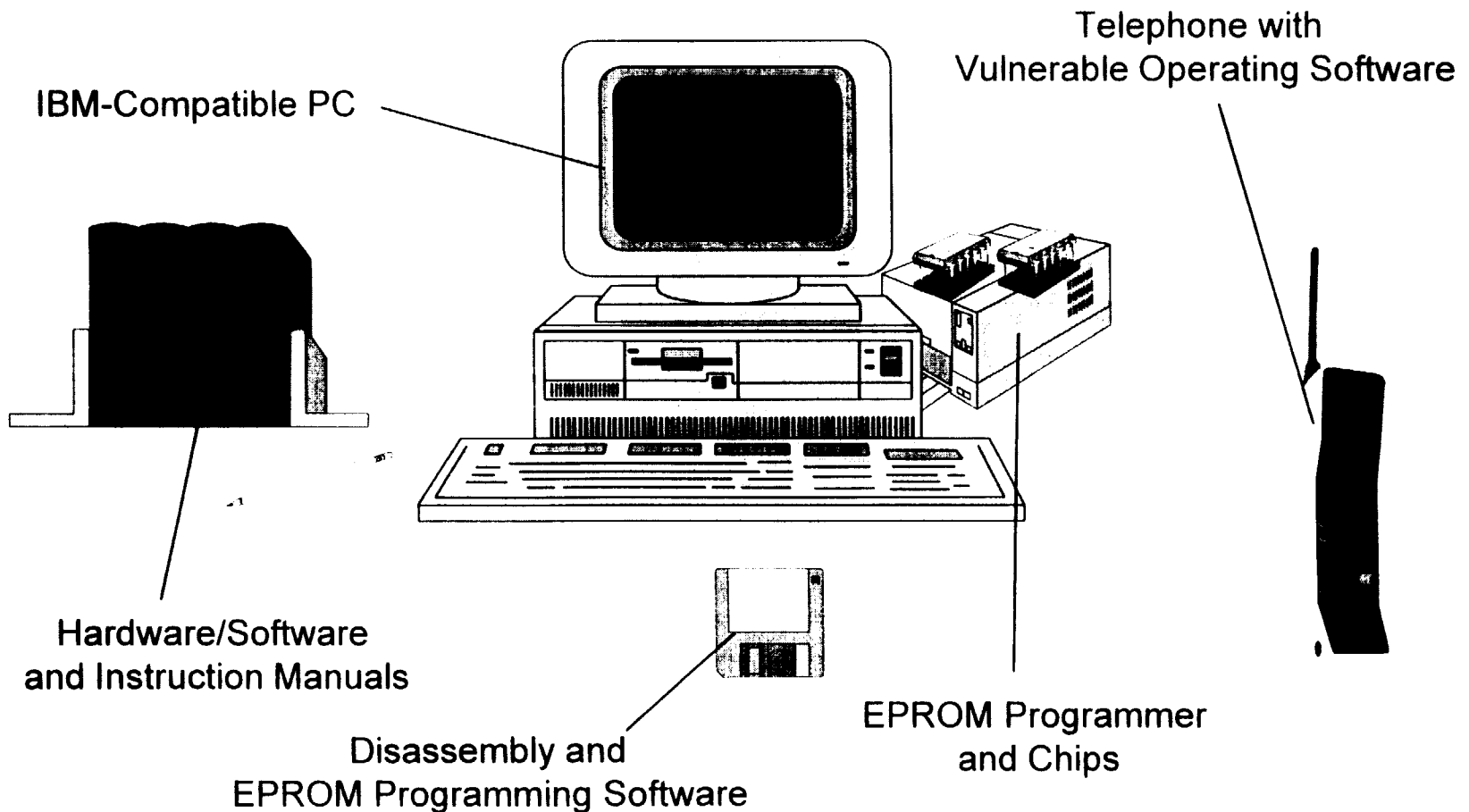# Typical Class C Counterfeiting

IBM-Compatible PC

Telephone with
Vulnerable Operating Software

Hardware/Software
and Instruction Manuals

Disassembly and
EPROM Programming Software
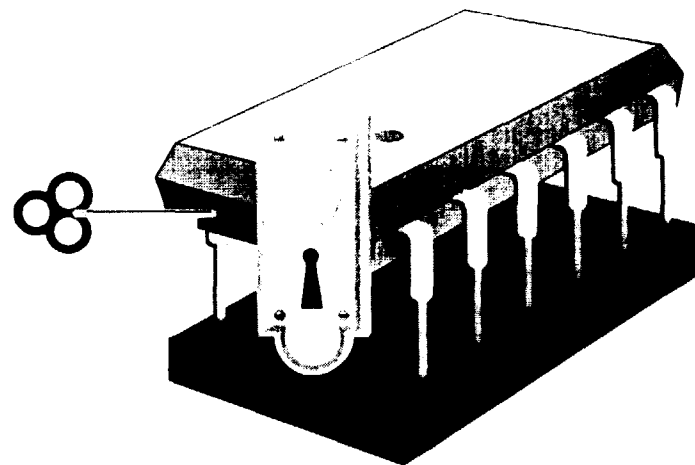
EPROM Programmer
and Chips

AT&T Wireless Services

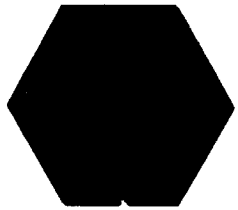# Technical Efforts to Enhance Telephone Security

ESN Storage

Firmware Storage

AT&T Wireless Services

Cellular Fraud Control – Locking the Radio Path

Central Office

Mobile Telephone Switching Office

Cell Site

700–3

AT&T Wireless Services

Why Reduce and Manage Fraud?

To decrease
financial losses

To decrease
network and
administrative costs

To keep good
customers happy

To prevent
bad image

AT&T Wireless Services

Balancing Fraud and Business Operations

Complexity
User Friendliness
Effectiveness
Reliability
Timeliness

Fraud Control Solutions

Performance Requirements

AT&T Wireless Services

Existing Technologies for Fraud Management

◆ **Pre-call validation of every call**

◆ **Post-call validation of every call**

◆ **Expert system-based call detail analysis systems (CloneDetector)**

◆ **Personal Identification Number (PIN) identification techniques – "Fraud Prevention Features"**

Fraud Products and Services

◆ **Profiling "CloneDetector" System**

◆ **FraudManager Service**

◆ **HLR Visibility**

◆ **Stolen Phone StatCheck Service**

◆ **Customer Positive File Service**

◆ **Positive Validation Service (PVS)**

Emerging Technologies for Fraud Management

◆ **Time-based validation systems**

◆ **Radio frequency (RF) signature technology**

◆ **Voice verification technology**

◆ **Dynamic password technology**

◆ **Cryptographic authentication techniques**
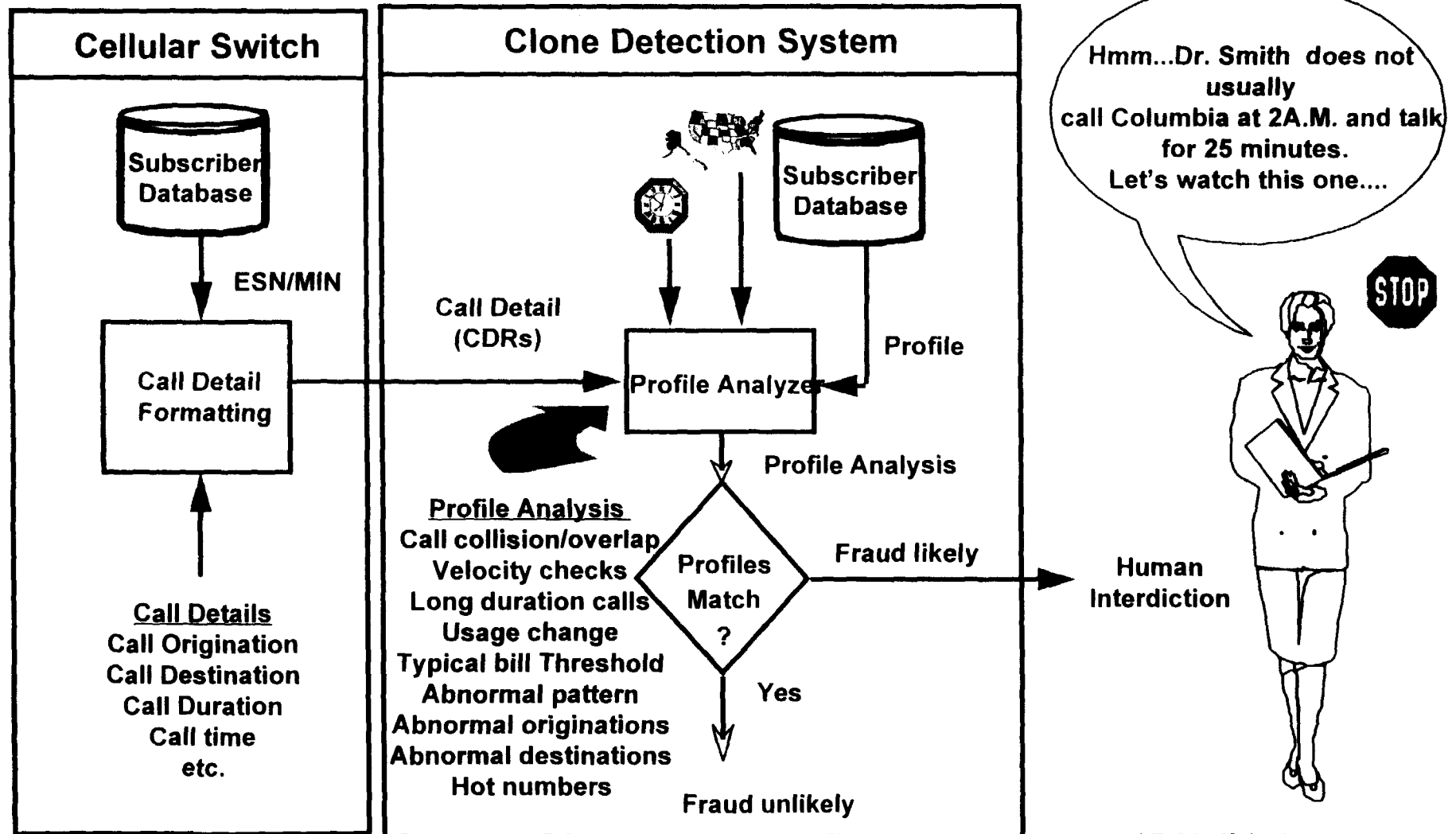
Principle of Profiling System

Cellular Switch	Clone Detection System

Subscriber Database

ESN/MIN

Call Detail Formatting

Call Detail (CDRs)

Subscriber Database

Profile

Profile Analyzer

Profile Analysis

Profile Analysis

Profile Analysis
Call collision/overlap
Velocity checks
Long duration calls
Usage change
Typical bill Threshold
Abnormal pattern
Abnormal originations
Abnormal destinations
Hot numbers

Profiles Match ?

Yes

Fraud likely

Human Interdiction

Fraud unlikely

Call Details
Call Origination
Call Destination
Call Duration
Call time
etc.

Hmm...Dr. Smith does not usually call Columbia at 2A.M. and talk for 25 minutes. Let's watch this one....

STOP

AT&T Wireless Services

Velocity Checking – An Example
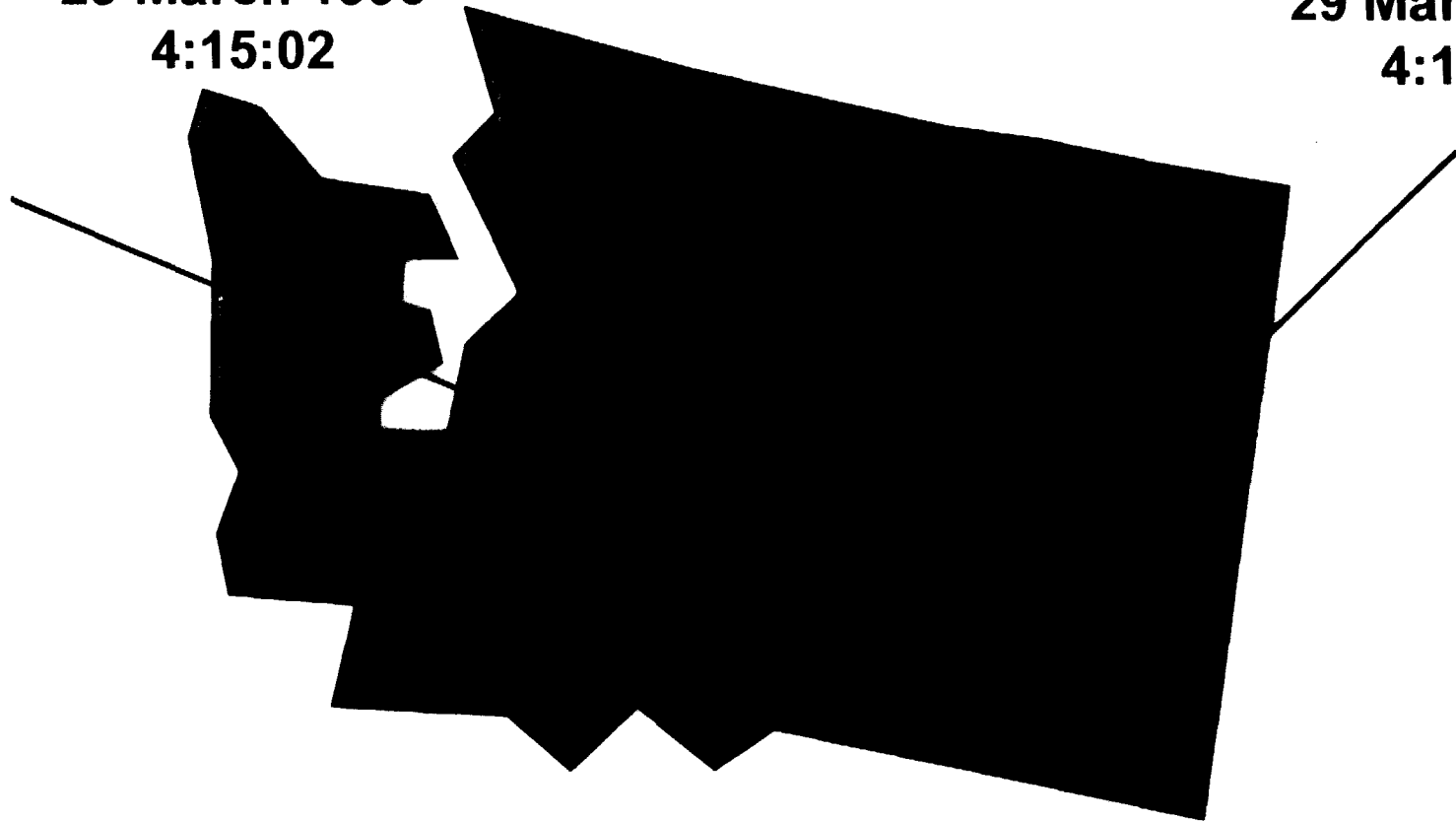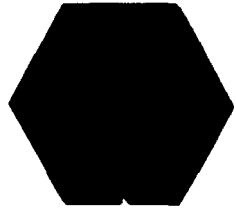
**Seattle
29 March 1996
4:15:02**

**Spokane
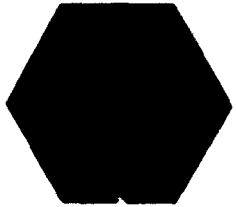29 March 1996
4:16:54**

RF Fingerprinting Technology - Per cell site

Database and Interdiction Unit

AT&T Wireless Services

Principle of Cellular Authentication Using Voice Verification

Cellular Telephone	Cellular Switch

Voice Challenge

Text Challenge

Voice Response

Text Response

Yes

No

User ID

User ID

User ID =
ESN, MIN, User

700–65

AT&T Wireless Services

Taxonomy of Fraud Control Techniques

```
                    ┌──────────────────┐
                    │  Fraud Control   │
                    │   Techniques     │
                    └──────────────────┘
      ◄──── Less Effective        More Effective ────►

┌──────────────────┐                    ┌──────────────────┐
│ Fraud Detection  │                    │ Fraud Prevention │
│   Techniques     │                    │    Techniques    │
└──────────────────┘                    └──────────────────┘

   ┌──────────────┐          ┌──────────────────┐   ┌─────────────────────┐
   │   Profiler   │          │    Weak Fraud    │   │    Strong Fraud     │
   └──────────────┘          │Prevention Techniques│ │Prevention Techniques│
                             └──────────────────┘   └─────────────────────┘
   ┌──────────────────┐
   │Intelligent Switch│         ┌──────────────┐      ┌──────────────┐
   └──────────────────┘         │  Static PINs │      │ Dynamic PINs │
                                └──────────────┘      └──────────────┘

                                ┌──────────────┐      ┌──────────────┐
                                │ Multiple PINs│      │Authentication│
                                └──────────────┘      └──────────────┘

                                ┌────────────────┐
                                │RF Fingerprinting│
                                └────────────────┘

                                ┌──────────────────┐
                                │Voice Verification│
                                └──────────────────┘
```
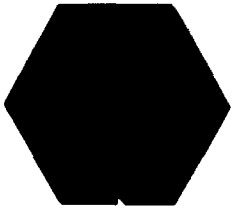
AT&T Wireless Services

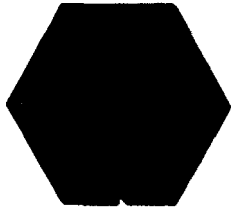# Cryptology — Basic Concepts

◆ **Cryptology**

— Science that embraces both cryptography and cryptanalysis
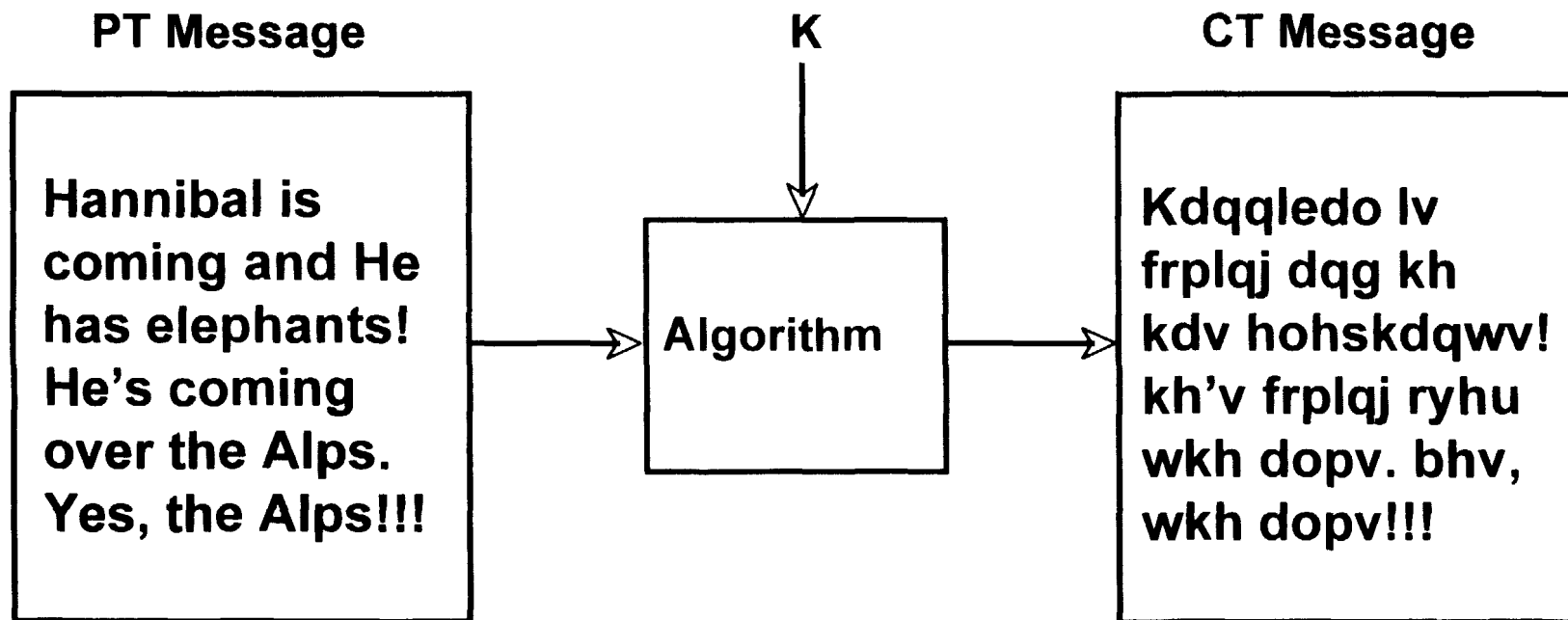
◆ **Cryptography**

— Art (or science) of secret writing

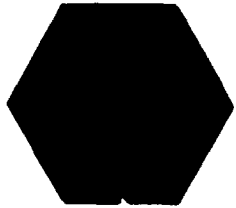— Includes means for performing all "security services"

◆ **Cryptanalysis**

— Attempt to descramble or scramble without knowledge of secret key

Example of Simple Cryptographic System

PT Message

K

CT Message

Hannibal is
coming and He
has elephants!
He's coming
over the Alps.
Yes, the Alps!!!

Algorithm

Kdqqledo lv
frplqj dqg kh
kdv hohskdqwv!
kh'v frplqj ryhu
wkh dopv. bhv,
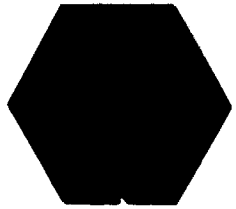wkh dopv!!!

700–90

History of Cryptography

- ◆ **Circa. 1900 B.C. — Birth of Cryptology**
  - — **Egyptians use hieroglyphic symbols to document history**

- ◆ **50 B.C.**
  - — **Julius Caesar writes to friend Cicero using the "Caesar alphabet"**

- ◆ **Middle Ages**
  - — **Geoffrey Chaucer uses symbol cipher in several works**

- ◆ **Late 1700's**
  - — **Thomas Jefferson — the Father of American Cryptography develops "cypher wheel"**

History of Cryptography (cont'd)

◆ **Civil War Period**

— **Armies use "word transposition" cryptography to protect military communications**

◆ **1926**

— **Vernam develops concept of "one-time pad" telegraph cipher**
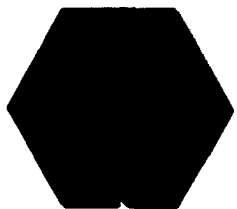
◆ **World War II Period**

— **U.S. uses Hagelin (Converter M-209) for military communications**

◆ **1974**

— **IBM develops Data Encryption Standard (DES)**
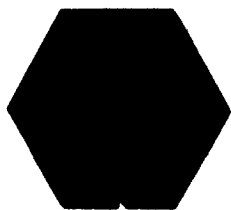
◆ **1995**

— **U.S. introduces authentication for cellular**

AT&T Wireless Services

Authentication ... A Closer Look

Authentication

Money Dispensing at ATM Machine — Everyday Authentication
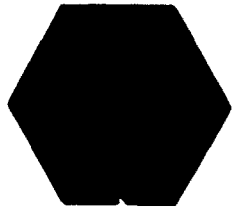
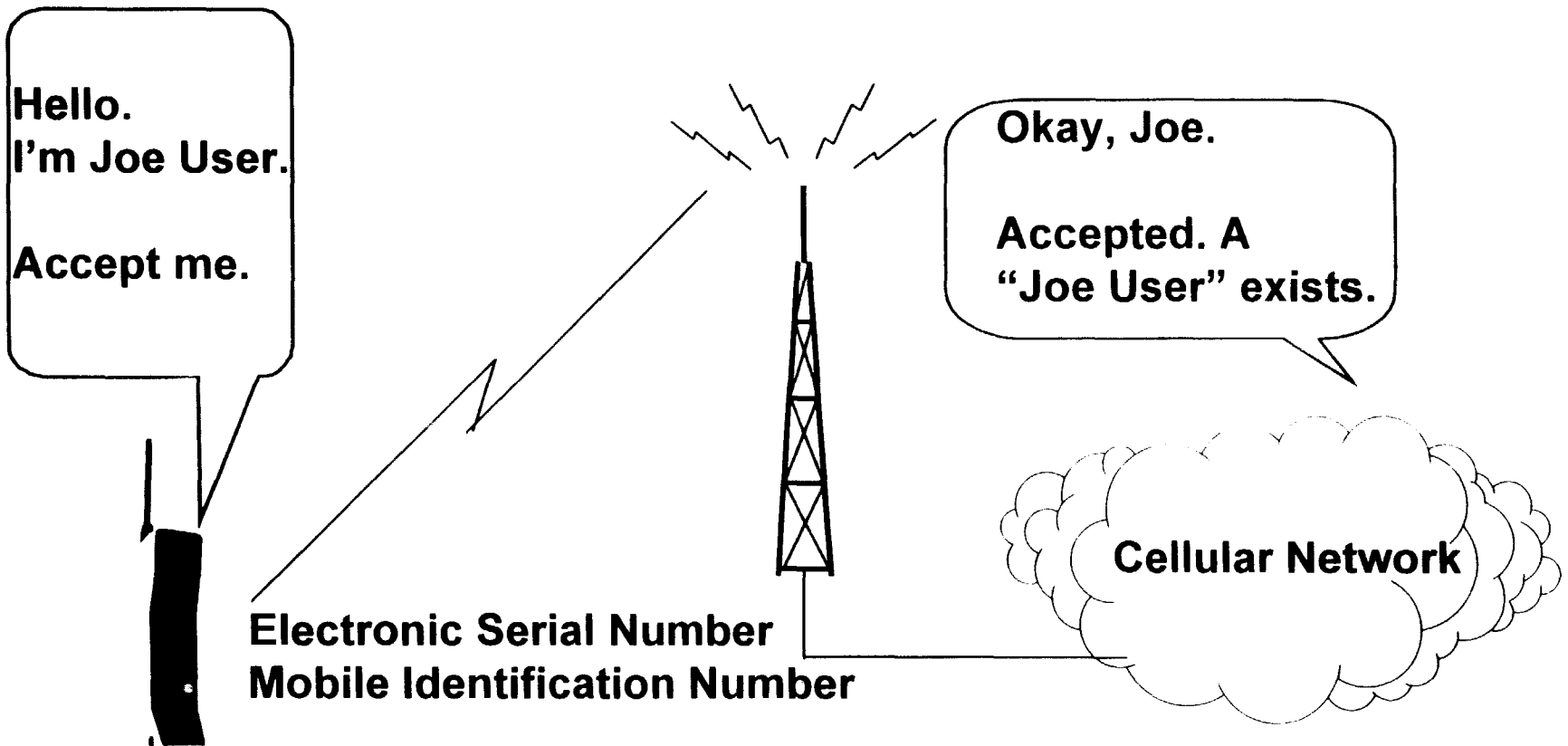# Fundamental Definitions

◆ Identification

— Process whereby the cellular network recognizes a subscriber's identity over the radiopath
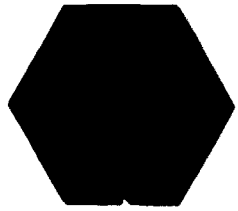
— Analogous to a computer *UserID*

◆ Authentication

— Process whereby the cellular network verifies the claimed identity of a subscriber to protect the network against unauthorized use (theft of service)

— Analogous to a password associated with the UserID

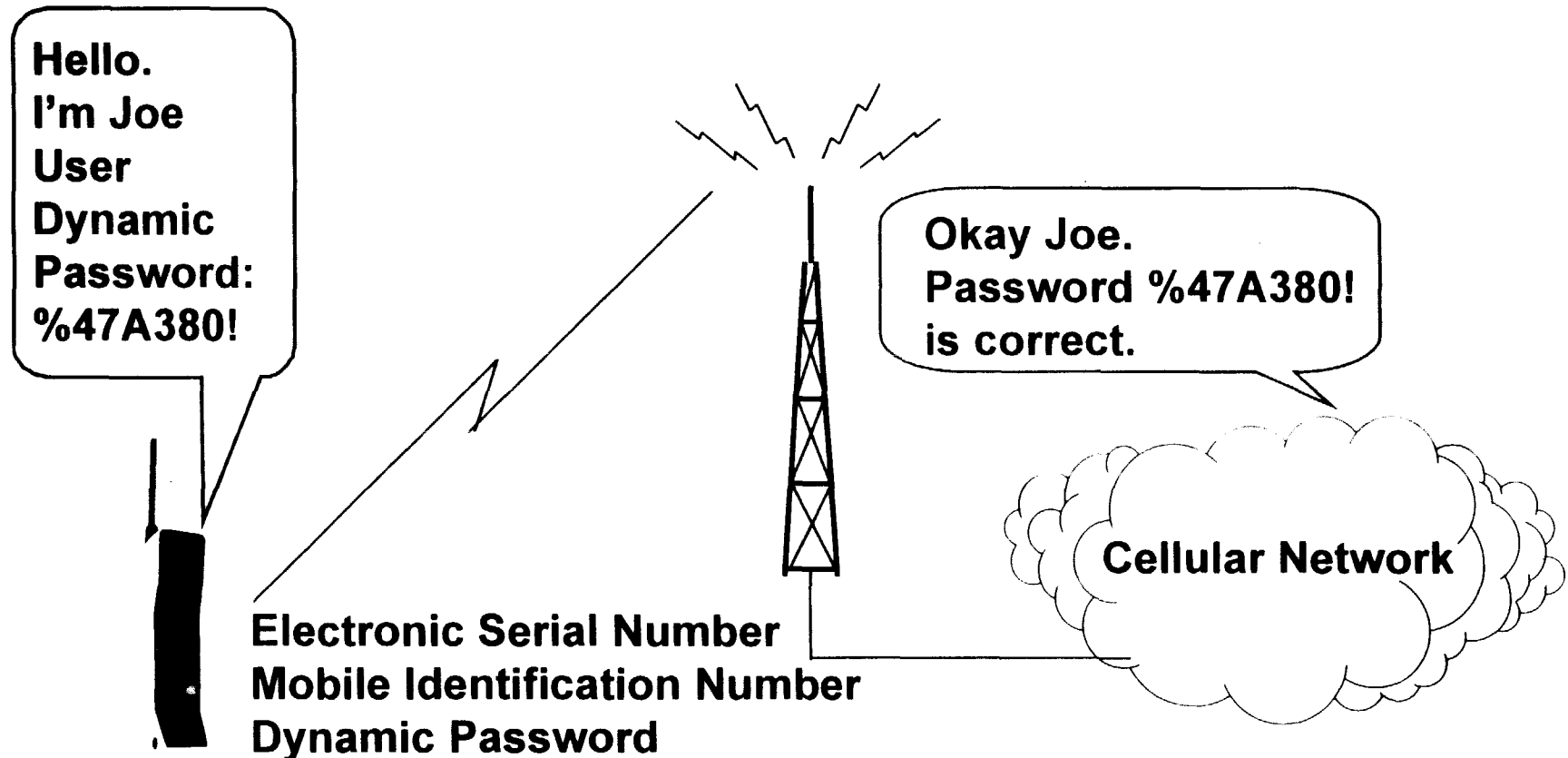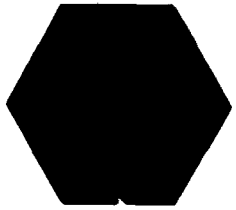— In the cellular environment, the password is "dynamic": changing on every access attempt

AT&T Wireless Services

Current Cellular "Identification" Scheme

Hello.
I'm Joe User.

Accept me.

Okay, Joe.

Accepted. A
"Joe User" exists.

Electronic Serial Number
Mobile Identification Number

Cellular Network

AT&T Wireless Services

Cellular Challenge-Response "Authentication" Scheme

**Hello.
I'm Joe
User
Dynamic
Password:
%47A380!**

**Okay Joe.
Password %47A380!
is correct.**

Cellular Network

**Electronic Serial Number
Mobile Identification Number
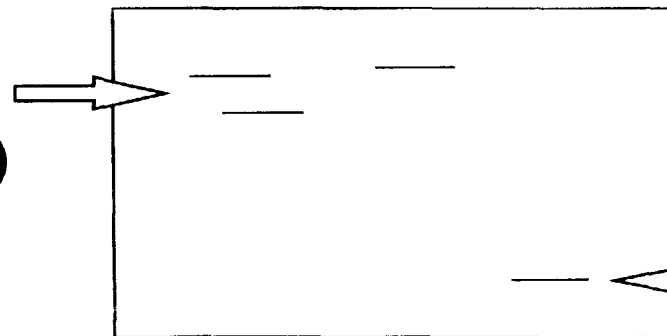Dynamic Password**

AT&T Wireless Services

Basic Principles of Identification, Friend, and Foe (IFF)

Interrogation - Coded "Challenge"
Transponder Reply - Coded "Response"

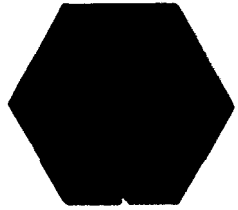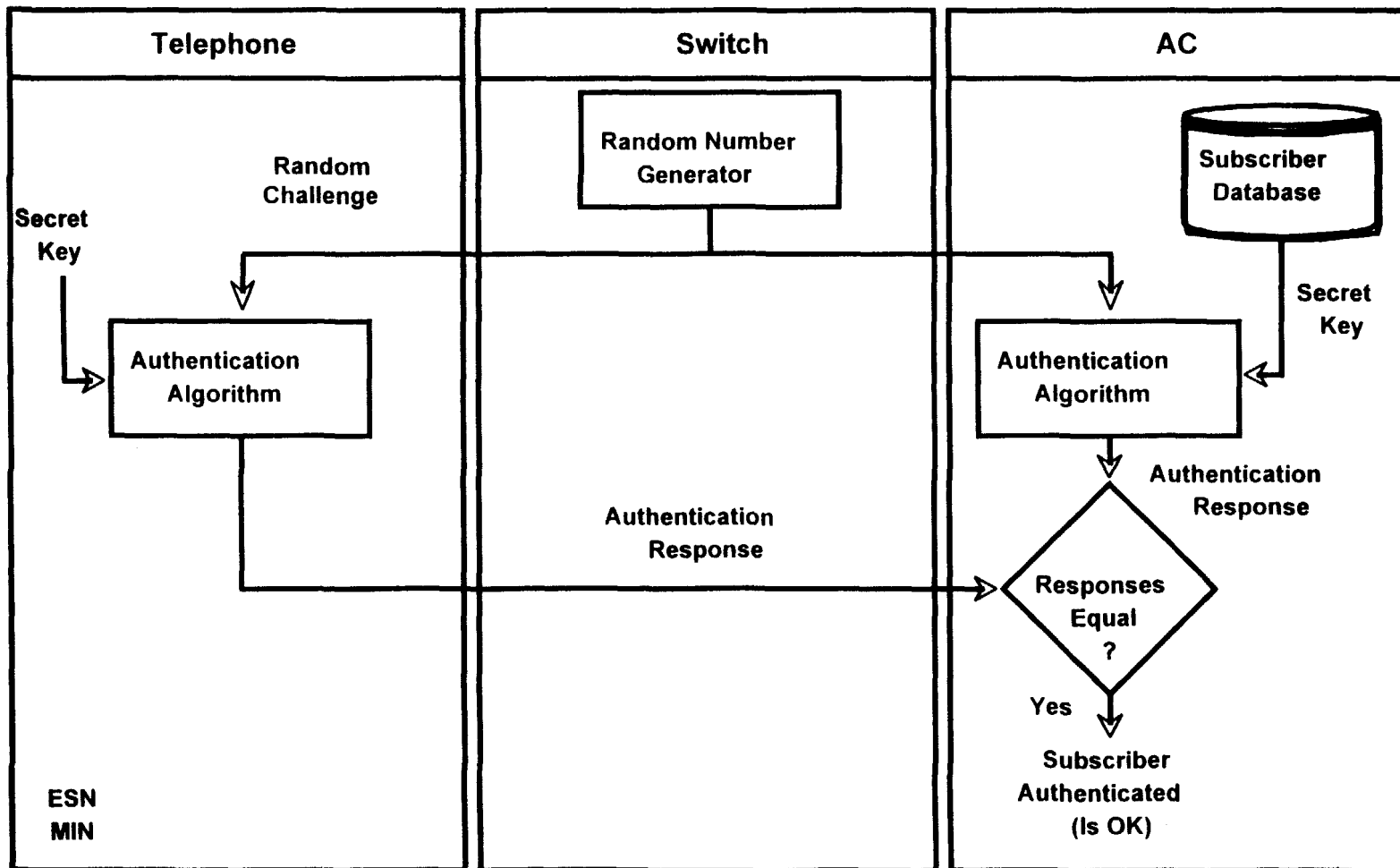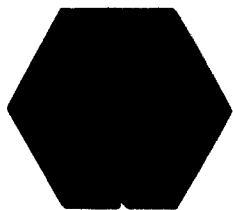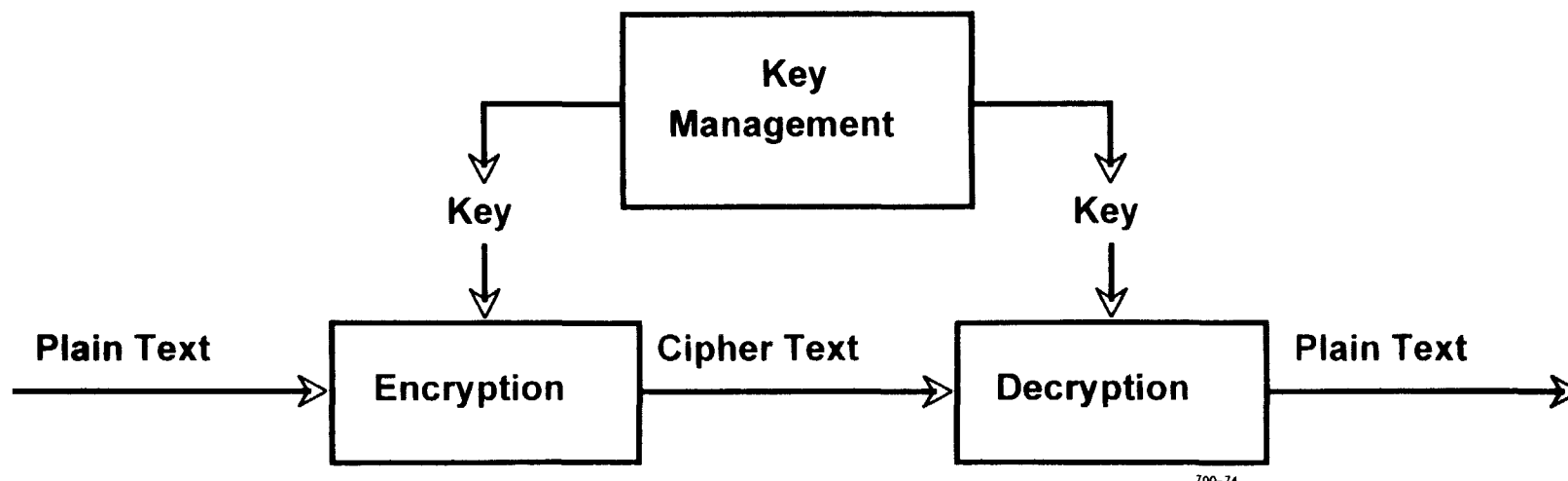**Radar Display**

Foe
(Unknowns)

Friend

Principle of Cellular Authentication

Telephone	Switch	AC

Telephone

Secret Key

Random Challenge

Authentication Algorithm

ESN
MIN

Switch

Random Number Generator

Authentication Response

AC

Subscriber Database

Secret Key

Authentication Algorithm

Authentication Response

Responses Equal ?

Yes

Subscriber Authenticated (Is OK)

700–63

AT&T Wireless Services

Cryptographic Key Management

"The generation, distribution/issuance, storage, updating, destruction, and archiving of keys"

AT&T Wireless Services